BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-209

10 NOVEMBER 1994

AIR FORCE MATERIEL COMMAND
Supplement 1

17 AUGUST 1998

Security

THE AIR FORCE RESOURCE PROTECTION PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: HQ AFSPA/SPLE (Capt Shawn I. Reilly)
HQ AFMC/SF (SMSgt Carl A. Eskew)

Certified by: HQ USAF/SP
(Col Steven R. Shoemaker)
HQ AFM/SF (Lt Col George G. Barr)

Supersedes AFI 31-209, 22 July 1994.
AFI31-209/AFMCS 1, 5 April 1996.

Pages: 53
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 31-2, *Law Enforcement.* It gives the requirements for the Resource Protection Program (RPP) and addresses the physical security of Air Force personnel, installations, operations, and assets. This instruction applies to all Air Force personnel, installations, and facilities located on lands under Air Force jurisdiction. It also applies to Government-Owned, Contractor-Operated (GOCO) or contractor-owned, contractor-operated (COCO) facilities. **Chapter 6**, **Chapter 7**, and **Chapter 8** do not apply to Air National Guard units and members.

(AFMC) Anyone desiring access to an AFMC installation is subject to the specific prohibitions and requirements of this supplement. Persons subject to the Uniform Code of Military Justice (UCMJ) who violate paragraph 5.1.3.6.1. (Added), 5.1.4 and its component paragraphs, are subject to punishment under Article 92, UCMJ. Civilian employees who violate this supplement are subject to civilian prosecution, and disciplinary action IAW applicable Air Force directives. Although specific resource protection guidelines do not apply to the Air National Guard or US Air Force Reserve units and members, the specific prohibitions and requirements of the supplement do apply.

SUMMARY OF REVISIONS

This revision allows MAJCOMs to delegate waiver and exception authority for protection of arms, ammunition, and explosives (AA&E) to installation commanders; and also clarifies procedures commanders must follow to ensure lost, stolen, unaccountable, or recovered US Government AA&E is reported to the installation chief of security police. Changed material is indicated by a | .

(AFMC) This edition is a significant revision containing policy and procedure changes. Designates AFMC installations as closed bases, authorizes storage of privately owned ammunition in Military Family Housing and in authorized government storage facilities. This supplement delineates armed escort requirements for AA&E movements, requires owner/user to provide armed surveillance during mobility processing, and establishes protection standards for Ground Wave Emergency Network (GWEN) Systems, and archaeological sites.

AFI 31-209, 10 November 1994, is supplemented as follows:

Chapter 1

RESPONSIBILITIES

1.1. Objective. The Resource Protection Program (RPP) has four primary objectives:

- Maintain the Air Force war fighting capability by reducing damage to Air Force resources.
- Safeguard Air Force property by reducing the opportunity for theft or terrorist attack by making a potential target inaccessible or unattractive.
- Promote the use of the Crime Prevention Through Environmental Design (CPTED) principles of natural surveillance, natural access control and territorial reinforcement.
- Ensure that everyone safeguards government property.

1.2. Headquarters United States Air Force, Chief of Security Police (HQ USAF/SP). Develops policy and provides oversight of the RPP.

1.3. HQ Air Force Security Police Agency (HQ AFSPA). Develops protection standards and monitors the effectiveness of the RPP.

1.4. HQ Air Force Intelligence Support Agency (HQ AFISA). Approves requests for deviations from protection standards for sensitive compartmented information (SCI) facilities (SCIFs).

1.5. Air Force Safety Agency. Approves all requests for deviations on terrestrial nuclear reactors in accordance with AFI 91-304, *Air Force Nuclear Reactor Program*.

1.6. Major Commands, (MAJCOM)/SP:

- Manage the RPP within their commands.

1.6. (Added-AFMC) Physical protection standards for governement owned-contractor operated (GOCO, also known as Air Force plants) facilities will conform to the standards in this Air Force instruction to the maximum extent possible based on individual plant characteristics, and as specified in appropriate contracts affecting individual facilities. Use AFI 31-703, *Product Security*, Attachment 1, for considering enhanced physical security features to be identified in contract provisions. Oversight of physical protection programs at Air Force plants is the responsibility of the Aeronautical Systems Center Acquisition Security Directorate according to AFI 31-703.

1.6.1. HQ Air Combat Command (HQ ACC). In addition to the responsibilities listed in Paragraph **1.6.**, HQ ACC/SP establishes protection requirements for the GWEN systems and OTH-B Radar.

1.6.2. HQ Electronic Systems Center (HQ ESC). In addition to the responsibilities listed in Paragraph **1.6.**, HQ ESC/AVJ serves as the Air Force point of contact for technical issues on IDE for the RPP.

1.7. Installation Commanders:

- Approve deviations and waivers of protective standards for all arms, annunitions, and explosives (AA&E) facilities.

- Develop and implement either an installation RPP (IRPP) or installation security plan (merging is acceptable).
- Establish a Resources Protection Executive Committee (RPEC).
- Designate controlled areas and storage facilities.
- Grant the authority to enter controlled areas. ***Note: Installation commanders may delegate this authority in a base directive to a unit, geographical separated unit (GSU), or site commander responsible for a specific area.***
- Grant or restrict entry into installations and authorize searches.
- Develop guidance on protecting privately owned firearms and other types of dangerous weapons.
- Establish local requirements for night depository or central depository, fund storage limits, and fund escort procedures.
- Approve waivers.
- Approve deviations from this AFI in accordance with treaties and agreements with foreign governments, allied forces, and continental United States (CONUS) civilian governments.
- Designate all additional installation responsibilities in writing.

1.8. Unit Commanders:

- Identify assigned mission-essential resources.
- Provide physical protection in accordance with the IRPP.
- Designate a unit focal point for RPP.

1.8. (Added-AFMC) Designate unit focal point in writing and furnish a copy of the appointment letter to the Chief of Security Forces.

1.9. Installation Chief of Security Police (ICSP):

1.9.1. Supervises the RPP by:

- Conducting program reviews and technical surveys.
- Publishing directives and developing plans.
- Coordinating RPP-related construction projects and contracts.
- Monitoring training of unit RPP focal points.

1.9.2. Enforces the RPP Directives and Contingency Plans by:

- Controlling installation entry.
- Monitoring IDE.
- Providing an armed response capability.
- Investigating incidents.

1.9.3. Manages the RPP by:

- Recording the minutes of the RPEC.
- Accomplishing program review reports.
- Controlling waivers and exceptions.

1.10. Resource Protection Program Manager:

- Oversees community-wide crime prevention consultation services.
- Processes criminal statistical data to examine crime patterns.
- Recommends crime prevention strategies.
- Provides analyzed crime data to unit commanders, law enforcement activities, and other interested agencies.
- Maintains liaison with civilian organizations and authorities.
- Develops media campaigns to publicize the base crime prevention program and crime problems.

1.10. (Added-AFMC) The resource protection manager (RPM) is:

- The focal point for resource protection program reviews.
- The installation focal point for training the base security managers/resource protection program focal points on program requirements. Specific training topics are:
- Circulation control.
- Physical security measures in use at the protected facility, organization, or activity.
- Incident reporting.
- Antirobbery procedures as applicable.
- Program review requirements.
- Other training requirements determined locally.

1.10.1. Child Fingerprint Program. As part of your crime prevention program, consider developing a child fingerprint program. Use the following guidelines when implementing this child identification program:

- A parent or guardian should normally be present during fingerprinting, but may designate, in writing, other adults to act in their behalf during the fingerprinting of their children.
- Use the DJFD Form 353, **Personal Identification**, for fingerprinting.
- Return all cards to the parent or guardian for safekeeping.
- Do not endorse or participate in fingerprinting programs that charge a fee for fingerprinting.
- Don't use fingerprint packets that must be purchased by parents for security police sanctioned fingerprint programs.

1.11. The Resource Protection Executive Committee (RPEC). The RPEC meets at least once a year. The installation commander selects committee members from major functional areas, including representatives from tenant organizations. ***Note: Small sites and operating locations organize the RPEC as determined by the MAJCOM.***

1.12. RPEC Working Groups. The RPEC working groups may establish working groups to address specific needs. Normally, functional specialists serve as members of RPEC. The chairperson designates the office of primary responsibility for each working groups. Determine membership based on the issues and problems. RPEC working groups:

- Identify mission-essential resources.

- Determine installation threats and draft appropriate protective standards.
- Test program effectiveness.

1.12.1. These are four common working groups:

- **Threat Working Group.** Normally composed of representatives from Air Force Office of Special Investigations (AFOSI), security police, and intelligence and is chartered to prepare the installation threat vulnerability assessment based on crime analysis, loss statistics, assessment of high risk facilities, and other data.
- **Loss Prevention Working Group.** This group is normally composed of technical representatives from various organizations and is charged to monitor the integrity of the base resource management system.
- **Plans Working Group.** Normally composed of technical representatives from security police, installation operations, plans, logistics plans, and intelligence plans. This group should develop, staff, coordinate, and prepare the IRPP.
- **Alarm Working Group.** Normally composed of representatives from security police, civil engineers, communications, and representatives from units with funds and AA&E storage requirements. This group is charged with reviewing the status of Intrusion Detection Equipment (IDE) and recommending priorities for resource allocation and maintenance. They also provide additional services as directed by the RPEC.

NOTE:

The chairperson may merge working groups.

Chapter 2

PROGRAM MANAGEMENT

2.1. The Installation Resource Protection Plan (IRPP). The Air Force concept is to provide the greatest degree of protection, for the greatest number of resources, for the least cost. The essence of the IRPP is to identify the resources, project the threat analysis against them, and develop realistic counter measures based on existing and programmed capabilities. Installation planners must have detailed information on resources that support emergency situations, contingencies, and transition into wartime. Refer to Air Force Manual 10-401, *Operation Plan and Concept Plan Development and Implementation*, for format and guidance for detailed preparation. This plan must include as a minimum:

- A threat estimate.
- A terrain and weather analysis of the installation and its surroundings.
- An assessment of the installation's vulnerability to terrorist acts or sabotage.
- A concept of operations for resource protection contingencies.
- An estimate of support resources from friendly forces.

2.1.1. Contingency Operation Requirements. Develop contingency operation requirements for these situations:

- Anti-hijack, anti-robbery, and anti-terrorist measures.
- Bomb threat, civil disturbance, and hostage situations.
- Mass casualty incidents, mobility, and NMSAs.
- Other mission-essential resources as determined by the RPEC.
- Resident and transient DVs, resources secured or protected by civilian (contract) police if work stoppages or walkouts occur.
- Develop specific contingency procedures for:
- Department of Energy nuclear shipments.
- AA&E shipments.
- All other shipments that require safe-haven status.

2.1.2. Planning Requirements. Installation planners must translate basic RPP requirements into local implementation procedures. Planners must be aware of:

- Basic RPP concepts.
- Mission-essential installation resources.
- Potential installation threats.
- For further information on how to implement risk management and CPTED, see the applicable AF Handbook 31 series.

2.2. Program Reviews. The RPP makes use of teams to evaluate the installation's protection needs and programs to support Air Force resources. The security police resource protection program manager coordinates two types of reviews, initial and follow-up. Program reviews:

- Determine whether the installation program adequately protects its resources from criminal activities (on-base and off-base) and terrorist acts.
- Recommend program improvements.
- Provide feedback for command action.

2.2.1. Initial Reviews. RPP teams conduct a detailed initial survey of the installation to assess protection requirements. All teams must include representatives from security police, civil engineering, and communications.

2.2.2. Follow-Up Program Reviews. RPP teams conduct follow-up reviews:

- Annually by the security police for all AA&E (Category II or higher).
- Biennially for areas containing major funds ($100,000 or more) and those areas approved for storage of controlled substances like pharmacies and other medical logistics supply facilities.
- As determined by the RPEC for facilities storing and handling funds less than $100,000.

NOTES:

During the off-year, the owner or user of all other controlled areas must conduct the follow-up program reviews and provide a completed copy of program review reports to security police.

- As determined by the RPEC on facilities storing and handling funds less than $100,000.

2.2.3. Program Review Reports. RPP teams may prepare program review reports for a single building, a facility, an entire remote site, GSU, or an installation. The review reports must include:

- Methods for indoctrinating personnel on circulation control procedures.
- An assessment of education and motivation programs.
- An assessment of physical protection for facilities and equipment.

2.3. Antirobbery Tests. The IRPP or security plan prescribes anti-robbery tests:

- Annually for all drug facilities and Category II or higher AA&E facilities at major funds levels ($100,000 or more).
- Periodically for other alarm-equipped facilities and customer service areas in relation to local threats, as directed by the RPEC.

2.4. Community Policing. Planners help develop a program for security police and the rest of the military community to work cooperatively in reducing crime. See applicable AF Handbook 31 series for key features of the program.

2.4.1. Operation Crime Stop Program. Installation commanders establish a base Crime Stop program for obtaining information on possible criminal activities from confidential sources. Commanders must protect the identities of these individuals according to AFI 37-132, *Air Force Privacy Act Program* and AFI 37-131, *Air Force Freedom of Information Act Program*.

2.4.2. Receiving Reports. The law enforcement desk must have a telephone line for reporting crimes in progress from both on- and off-base. Bases with on-line access to local 911 Emergency Reporting Systems may choose to use that system as their Crime Stop hotline.

2.4.3. Recording Calls. Log each Crime Stop call on an AF Form 53, **Security Police Desk Blotter**, beginning each entry with the words **Crime Stop.** Security police keep records on the number of calls received and the results of police response.

2.4.4. Setting Up the Field Interview Program. Use field interviews in specific instances of reported or suspected crimes. Use the field interview card to document contact with suspicious persons. Provide this data to the security police investigation's section.

2.4.5. AF Form 1608, Emergency Numbers Telephone Decals. Place this form on the telephone for personnel to use in emergencies.

2.4.6. AF Form 440, Bomb Threat Aid. Use this form to help gather information on bomb threats.

2.4.7. AF Form 1670, Valuable Property Record. Use this form to record serial numbers and all other pertinent descriptive data for high value property.

2.5. Installation Entry Policy. Installation commanders set up entry and internal controls to deter unauthorized people from entering an installation. Make sure that these controls allow authorized personnel to enter and leave the base efficiently.. The IRPP or security plan must outline unique entry for contingency operations.

2.5. (Added-AFMC) Installations may use AFMC Form 387, **Air Force Materiel Command Identification Credential**, and AFMC Form 496, **Application for AFMC Identification Card.** Use for personnel having a valid requirement for installation entry (contractors and others) who do not have a standard Air Force identification card. Installations will establish a system to control issue of the AFMC Form 387.

2.5.1. Levels of Control. Commanders determine the level of entry controls using these factors:

- The threat to the installation and local environment.
- The security priority of assigned resources as specified by AFI 31-101.
- Any pilferage problems specific to the installation. (Pilferage is the deliberate taking of property through circumvention of human controls and physical protection measures.)
- Base features that might present significant hazards to public safety.

2.5.2. Minimum Controls. Implement these minimum controls at every Air Force installation:

- Fence the installation perimeter, as determined by the RPEC.
- Operate only the minimum number of perimeter gates required for operational needs.
- Locate warning signs in these areas:
  - Entrances to the installation.
  - The perimeter of the installation.
  - The boundary and entrances to a controlled area (camouflaged tactical areas excluded).

NOTE:

See paragraph **9.5.** for a list of visual aids authorized by this directive.

2.5.2. (Added-AFMC) Normally, AFMC installations will have perimeter fencing. In those instances where fencing is impractical or not cost effective due to geographic or terrain features (i.e.,

remote locations, swamps, rugged mountainous terrain), installation location, mission uniqueness, or other circumstances, the installation commander may waive fencing requirements. The installation commander will conduct a risk assessment identifying vulnerabilities in the installation/resource protection plan. Compensatory force protection measures will be developed to ensure adequate security of the perimeter during increased THREATCONS and enhanced security operations.

2.5.2.1. For those areas under government control where the Air Force does not exercise federal exclusive jurisdiction, the local staff judge advocate makes recommendations concerning the use of lands and controlled areas based on local statues.

2.5.2.1. (Added-AFMC) When practical, USAF GOCO facilities/plants will use warning signs to mark entry points and exterior boundaries. Required sign wording is in attachment 4. (Added).

2.5.3. Closed Bases. The USAF designates installations as closed bases when any one of these factors apply:

- The base routinely stores or supports priority resources (See AFPD 31-1, *Physical Security*).
- The base has excessive or serious theft problems.
- The base faces a highly significant and unique resource protection, terrorist, or security threat.
- The base can't confine features or activities posing significant public safety hazards to controlled areas.

NOTE:

Appropriately armed security police must staff all entry control points on a closed base.

2.5.3. (Added-AFMC) AFMC installations are normally designated closed bases. If the installation/center commander elects to open their base they will develop a plan identifying compensatory force protection measures ensuring adequate security of the installation. This plan may be an annex to the installation security/resources protection plan (ISRPP) and will be forwarded to AFMC/CC for approval.

2.5.4. Unauthorized Entry. Under Section 21 of the Internal Security Act of 1950 (50 United States Code (U.S.C.) 797, any directive issued by the commander of a military installation or facility, which includes the parameters for authorized entry to or exit from a military installation, is legally enforceable against all persons whether or not those persons are subject to the Uniform Code of Military Justice (UCMJ). If unauthorized entry occurs, security police:

- You may detain violator(s), order them to leave, or escort them off the installation.
- Properly identify violators.
- You may apprehend or remove violators who reenter an installation after the violator has been ordered to leave by an officer or person in command or in charge. Military officials may prosecute these violator(s) according to Title 18, U.S.C. 1382.

NOTE:

Civil law enforcement authorities also have the power to arrest and prosecute for unauthorized entry to government property. Always consult with the staff judge advocate when deciding jurisdiction issues.

2.5.5. Expulsions. Acting within the authority listed in paragraph **2.5.4.**, installation commanders may deny access to the installation through the use of a barment system. Barment orders should in

writing (See **Attachment 2**) but may also be oral. Security police maintain a list of personnel barred from the installation and those denied on-base driving privileges. Update the lists following local procedures.

NOTE:

Lists are For Official Use Only (FOUO). Don't allow the public to see these lists.

2.5.6. Installation Entry Point Checks. The installation commander determines when, where, and how to implement random checks of vehicles or pedestrians. The commander may delegate this authority to his/her vice, deputy or military magistrate appointed pursuant to Military Rules of Evidence 315 (d)(2). The commander conducts random checks to protect the security of the command or to protect Government property. Don't conduct checks merely for probable cause. Bases may use a locally devised computer program that randomly selects entry point checks. The installation commander and the staff judge advocate must approve this program quarterly.

2.5.7. Gate Closure Devices and Procedures. Installation commanders, with advice of the RPEC, install gate closure devices. Develop specific procedures for personnel to react to alarms or other emergencies.

2.5.8. Installation Vehicle Entry Points. Install protective vehicle deflectors at all entry points. All routine pedestrian and vehicular traffic must enter the installation entry points staffed by security police.

2.5.9. Special-Purpose Gates. Personnel trained by the base security police (including contractors and owners or users) may open and staff the base's special purpose gates. Close and lock these gates during periods of low volume traffic.

2.6. Enforcing Order Within or Near Air Force Installations:

2.6.1. Legal Aspects of Confrontation Management. The basic authority for all law enforcement actions rests with the Constitution of the United States, Article 4, Section 3. Commanders act on the authority delegated to them by Congress, as stipulated by Section 21 of the Internal Security Act of 1950 and DoDD 5200.8, *Security of DoD Installations and Resources*, 25 April 1991.

2.6.2. Law Enforcement Aid. The Posse Comitatus Act allows Federal forces to protect United States government property or officials against violence or forcible obstruction of their duties in time of war or national emergency. The act also allows the military to provide humanitarian aid during natural disasters.

- The President's authority to use Federal military forces under Title 10 U.S.C. Sections 332 and 333, 1982 edition is allowable by this act.

2.7. Civil Disturbance Intervention and Disaster Assistance. The authority to intervene during civil disturbances and provide aid during disasters is bound by the directive issued by competent authority rather than the decision of the installation commander. States must request Federal military intervention or aid directly from the President by the state's legislature or executive. Installation commanders must immediately report these requests in accordance with AFI 10-801, *Air Force Support to Civil Authorities* (formerly AFR 55-35).

2.7.1. Using Military Personnel. United States military personnel may intervene in disturbances in overseas areas as specified by host-nation law, bilateral agreements to which the United States is a party, and international pacts. It is USAF policy to make every reasonable effort to avoid any confrontation between United States military forces and host-nation demonstrators or other dissidents posing a potential threat to USAF resources. Local plans to counter such events must include provisions to request host-nation civil or military support as quickly as possible.

2.8. Command Authority. Under Section 21 of the Internal Security Act 1950 (50 U.S.C. 797), any directive issued by the commander of a military installation or facility (including a directive that authorizes entry to or exit from a military installation) is legally enforceable against all persons whether or not those persons are subject to the UCMJ. See also Greer vs. Spock, 96 S. Ct. 1211 (1976).

2.9. Enforceability. DoDD 5200.8, which implements Title 50, U.S.C. 797, delegates the authority to publish such directives to the commander of any MAJCOM, numbered air force, air division, wing, group, or installation. Any directive issued by a properly designated Air Force commander is enforceable against persons' subject to the UCMJ who were under that commander's jurisdiction.

2.9.1. Although Title 18, U.S.C. 1382 doesn't specifically pertain to protecting Air Force physical resources, this law makes it a criminal act for any person to reenter an installation after being removed from it (or ordered not to reenter it) by the installation commander, or a designated representative acting on specific instructions.

2.9.2. Outside the United States and its possessions, a commander's right to exercise authority comes from a combination of United States laws that apply in the overseas area and from bilateral and multilateral agreements between the United States and host countries concerned.

2.10. Legal Requirements. To have legal effect, all directives that commanders issue to protect the Air Force's physical resources must meet these requirements:

2.10.1. According to Title 50, U.S.C. 797 and DoD Directive 5200.8 these directives must:

- Be published by commanders designated by the Secretary of Defense in DoDD 5200. 8, Paragraph III.C.
- State specifically that the commander is issuing the directive in accordance with the *Internal Security Act of 1950* (50 U.S.C. 797) and pertains to one of the subjects listed in the act.
- Describe and identify the controlled area, and prohibit anyone from entering the area without the consent of the installation commander.

2.10.2. Directives which apply only to persons who are subject to the UCMJ must:

- Be issued by an Air Force commander, as defined in DoDD 5200.8, paragraph III.C (preferably by the installation commander who is responsible for the Air Force physical resources in the area).
- Clearly describe, locate, and identify the controlled area, and prohibit anyone from entering the area without the consent of the commander who issued the order.
- Clearly mark each controlled area and publicize the regulation to ensure all military personnel know of its existence.

2.10.3. Unit commanders must develop written procedures that have legal effect. The installation commander (or designee) should issue the order in writing to remove persons from the installation and direct them not to reenter.

2.10.4. Any directive that applies to persons in an overseas area who are not subject to the UCMJ must be consistent with any formal United States agreement with the host-nation. When a criminal offense occurs over which the United States has extra territorial jurisdiction, United States Federal authorities may prosecute a non-United States citizen offender.

Chapter 3

EQUIPMENT AND FACILITIES

3.1. General Information. Implement measures to protect Air Force equipment and facilities by carefully integrating staffing requirements, procedures, and physical protection elements (fencing, lighting, locks, IDE, and so on).

3.1.1. Programming Concepts. The RPEC and each commander must use a systems approach in the analysis of physical protection requirements to make sure all elements of the RRP are integrated and complement each other. The RPEC must consider the cost of physical protection standards and weigh these costs against other factors, such as sensitivity, criticality, vulnerability, location, and mission of the installation, facility, or resource.

3.2. Fence Construction and Lighting Criteria. Follow fence and lighting criteria in DoD 5100.76-M (for AA&E facilities) and Air Force Manual (AFMAN) 31-224, *Resource Protection/Security, Facilities, and Equipment*.

3.2.1. Security personnel may set up temporary barriers by posting the area boundary and restricting entry with a rope barrier.

3.3. Backup Power. Some resources of special sensitivity must have a backup power source. The RPEC identifies backup power requirements to the base civil engineer (See AFI 32-5009, *Operation and Maintenance of Electrical Power Systems*).

3.4. Intrusion Detection Equipment (IDE). IDE funding is normally the responsibility of the organization that owns or is the primary user (owner/user) of the facility or equipment requiring IDE. Base installation sensor systems (BISS) components are acceptable substitutes for Joint-Service Interior Intrusion Detection System (J-SIIDS) components. Air Force T.O. 31S9-4-1-111, *Selection and Application of Joint Services Interior Intrusion Detection System (J-SIDE)*, to decide which components are best for a particular application.

3.4.1. Selecting IDE. For help in selecting a suitable IDE system, contact HQ ESC/AVJ. Coordinate all requests for modifications or alterations to J-SIIDS (or the DoD standard IDE system) through the MAJCOM/SP and HQ ESC/AVJ.

3.4.1. (Added-AFMC) Send a memorandum to HQ AFMC/SFOI, Building 266, Room N208, 4225 Logistics Ave., Wright-Patterson AFB OH 45433-5760, outlining modifications/alterations to sensor systems.

3.4.2. Obtaining Additional IDE Guidance. Owners/users must follow guidance contained in DoD 5100.76-M, **Chapter 3** and DoDD 3224.3, *Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing Evaluation, Production, Procurement, Deployment, and Support*, Feb 17, 89, for all alarm systems. For SCIFs, use Director of Central Intelligence Directive (DCID) 1/21, *Manual for Physical Security Standards for Sensitive Compartmented Information Facilities*.

3.4.3. Using Leased or Purchased Equipment. Discourage contractors from using leased equipment or purchasing IDE that isn't a DoD-approved system. All commercially leased or purchased IDE must meet or exceed all DoD and Air Force equipment design and performance specifications. Before

acquiring any commercial IDE or component, follow the coordination process outlined in Paragraph 3.4.1.

3.4.4. Replacing IDE. The normal life of IDE is about 10 years. Plan to replace the system accordingly. Use the Alarm Working Group and the RPEC as the vehicles for long-term planning and integration issues. The system user must pay for the IDE.

3.4.5. Managing IDE. Security police manage IDE and duress systems. The base civil engineer manages the design, installation, modification, and maintenance of J-SIIDS only. However, consult with the civil engineer when designing all detection systems. The local communications unit provides and maintains adequate telephone line support.

NOTE:

When acquiring for commercial systems, be sure that the contract covers the system's installation, modification, and maintenance.

3.4.5. (Added-AFMC) When acquiring commercial sensor systems, units must purchase an all-encompassing maintenance contract or enter into a written agreement with base civil engineers stipulating their intention to maintain the system.

3.4.6. Testing IDE:

- The owner/user must conduct quarterly tests of all alarms with the alarm monitor (see the applicable AF Handbook 31 series for testing procedures).
- Use AF Form 2530, **Alarm System Test Record,** to document these checks. Verify this record during inspections or when directed by the installation commander.

3.4.7. Posting IDE Warning Signs. For all facilities protected by IDE, post AFVA 125-20, *Warning!! This Facility is Protected by an Intrusion Detection Alarm System. Warning??.* Mark the entry points of large facilities containing numerous IDE, such as nonnuclear munitions' storage areas (NMSA).

3.4.8. Unit Requirements. Units with IDE must follow these procedures:

- Specify, by letter to the security police, who may activate or deactivate alarm systems and who may pick up authentication codes.
- Ensure the letter is current by updating the data each time the list of personnel authorized to access the system changes.
- Provide personnel to guard the area if the IDE fails.

3.4.8. (Added-AFMC) Unit will contact the Law Enforcement (LE) desk and inform the controller who [individual(s) name and rank] will be guarding the facility/area while the sensor system is down. If possible, especially in the nonnuclear munitions storage area (NMSA), issue security forces (SF) radios to the unit for communication purposes.

3.4.9. IDE Protection Requirements. Users must keep the Control Unit (local intelligence unit) for J-SIIDS, Integrated Commercial Intrusion Detection System (ICIDS), Commercial Interior Intrusion Detection System (CIIDS), or any locally procured system inside the alarmed area. If the system includes an intelligent key pad (a pad that allows users access to the facility with a card or personal identification number), locate it outside the alarmed facility. All intrusion detection systems must

include a line supervisory capability equal to the value, sensitivity, and technical sophistication of the resource being protected.

3.4.10. Using Alarm Verification Codes. Develop and use an identification verification or duress code system when entering alarmed facilities, safes, or vaults.

3.4.11. Logging Openings and Closings of Alarmed Facilities. Security police log the opening and closing of alarmed facilities on AF Form 53 or on a computer file.

3.4.12. Nuisance Alarms. Installation commanders must implement a program to identify causes of nuisance and false alarms. Owners/users of alarm facilities maintain a log of all nuisance or false alarms for a 90-day period. Maintenance personnel analyze this data and determine the necessary corrective action. The log must record:

- The time and date that the alarm went off.
- The cause of the alarm (if known).
- The action taken (maintenance called or responded, reset without problem, and so on).

3.5. Electronic Entry Control Systems (EECS) and Advanced Entry Control Systems (AECS).

The Air Force doesn't classify electromechanical locks, mechanical locks, and other automated entry control systems that use a number or letter sequence combination as protection devices. These devices are a convenience for on-duty personnel for controlling entry to high-use controlled areas. For a full discussion of EECS and AECS, see AFMAN 31-224.

Chapter 4

CONTROLLED AREAS

4.1. Controlled Areas. Commanders may further protect areas that contain valuable resources by designating them as controlled areas. Only specified personnel may gain limited access to these legally defined areas.

4.1.1. Limit controlled area designations to those areas requiring additional protective measures beyond the base's required positive circulation controls.

4.1.2. Installation commanders must control entry to storage areas containing mission-essential resources not covered by AFPD 31-1. These storage areas include:

- Warehouses storing aircraft or weapons systems spare parts.
- Areas where personnel process large volumes of classified material.

4.1.3. Don't use a controlled area designation as a substitute for positive circulation control within the area. Don't designate these areas as controlled:

- Areas that provide adequate protection through proper employment of circulation controls.
- Areas that don't need the legal boundary provided by the controlled area designation.

4.2. Entry to Controlled Areas. Only personnel who have proper qualification and authority may enter controlled areas.

4.2.1. Entry Qualification. The installation commander determines the basic entry qualifications and publishes them in a base directive. Implement local entry control techniques, including personal recognition, cipher locks, badges, or AECS.

4.2.2. Parking Areas. Establish parking areas for privately owned vehicles outside of controlled areas whenever possible, consistent with operational necessity.

4.2.3. Controlled Area Badges. The RPEC determines if a badge system is essential to identify persons in controlled areas. When the RPEC mandates badges, develop local procedures to issue and control the badges. The owner or user of the controlled area must oversee the badge system. The RPEC may approve the AF Form 1199, CS, **Restricted Area Badge,** series, follow the guidance in AFI 31-101 with these exceptions:

- Waive the security clearance requirement for escorted officials (if this requirement exists).
- Don't impose a security clearance requirement for controlled areas unless directed by the responsible activity.
- Consider using a different series of the AF Form 1199 than the one used for restricted areas on the installation.

4.3. Controlled Area Entrances. Keep entrances to the minimum necessary for safety and operational control. Post signs indicating the controlled area in conspicuous and proper places, except when a sign would compromise the security of a controlled area. Use Air Force Visual Aids (AFVA) 31-203, *Controlled Area Sign (18 x 15),* 31-204, *Controlled Area Sign (36 x 30),* or 31-205, *Controlled Area Sign (5 x 7),* to mark these areas.

4.3. (Added-AFMC) USAF GOCO plants/facilities will post controlled area signs where required. Required sign wording is in attachment 5. (Added).

4.4. Establishing Controlled Area Free Zones. Establish free zones when construction projects or other temporary work activities make escort procedures impractical. Follow these general guidelines:

- Allow entry to the project work area a some point on the boundary of the controlled area with a free zone corridor. ***Note: If the free zone adjoins the exterior of the controlled area, provide entry control to limit access to contractors or approved base personnel.***
- Ensure that the responsible activity maintains surveillance over the boundary of the free zone as determined by the installation commander and ICSP.
- Close the free zone and secure the controlled area after normal project work hours.

4.4.1. Free Zones for Contractors. Send the contractor a letter describing the procedures for using the free zones during the project. The installation commander or designee must sign the letter.

Chapter 5

PROTECTION OF ARMS, AMMUNITION AND EXPLOSIVES (AA&E)

5.1. Firearms Protection Philosophy. Firearms of all types are susceptible to theft. Certain military unique firearms, because of their great casualty potential and their non-availability in commercial markets, are particularly susceptible. All commanders and supervisors must place continuing special attention and emphasis on protecting firearms. Installation commanders and, the RPEC must closely scrutinize the number and location of all firearms storage facilities on their installation with the goal of reducing and consolidating facilities where possible. Use government-owned facilities to store:

- Government-owned firearms.
- Firearms in the custody of Air Force nonappropriated fund activities.

5.1.1. Only remove firearms from a designated storage area for as short a time as possible and in small quantities. Privately owned firearms may be stored in government facilities for installation residents as determined by the installation commander. Complete the AF Form 1314, **Firearms Registration**, for each privately owned firearm maintained in a government facility.

5.1.1. (Added-AFMC) Storage of privately owned ammunition (POA) and firearms in licensed government owned storage facilities is authorized. The armory is a licensed storage facility. POA must be segregated from government owned ammunition. Develop local inventory procedures for POA/firearms. POA and firearms may be stored in military family housing (MFH). Storage of POA, reloading components, or firearms in single bachelor (airman/NCO/officer) quarters or temporary lodging facilities (i.e., TLF, VOQ, VAQ, etc.) is prohibited. NOTE: No black powder may be stored in licensed facilities. Muzzleloaders may store "Pyrodex" as a suitable substitute. Pyrodex is a class/division 1.3. Black powder is a high explosive class/division 1.1. Residents of MFH will contact their local fire chief for specific guidance (amounts allowed) in storing black powder, pyrodex, and smokeless powder. Residents of MFH who store reloading components or POA will notify their local fire department of such storage.

5.1.1.1. (Added-AFMC) All personnel residing on-base and not living in MFH will store their privately owned weapons and ammunition in the SF armory or other designated storage facility. Commanders must determine the need for unit personnel to have access to privately owned weapons. Based on reasonable cause, access to weapons may be denied and removed. In making a determination on reasonable cause, unit commanders shall consult the staff judge advocate, and prepare a memorandum of their conclusions. Unit personnel may have their commander’s decision reviewed by the commander's superior. Commanders authorize removal of privately owned weapons from the SF armory by letter. Implement controls for checking out weapons for specified periods of time, and employ measures to trace weapons not returned at the end of the checkout period. When unit commanders have reasonable cause, they may require unit personnel (residing in MFH) to store their privately owned weapons in the SF armory or other designated storage facility.

5.1.2. (Added-AFMC) Use DoDM 5100.76, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives,* to identify risk categories for weapons.

5.1.3. (Added-AFMC) Commander Responsibilities for Privately Owned Weapons. Installation commanders must employ measures that control privately owned firearms on their installation. They must:

5.1.3.1. (Added-AFMC) Specifically prohibit storage of firearms in male or female bachelor living quarters, including transient quarters.

5.1.3.2. (Added-AFMC) Except as expressly authorized in this supplement specifically prohibit concealment of all privately owned weapons, firearms, and dangerous nonfirearms on the installation. Examples of concealment: hiding a firearm or dangerous weapon on one's person; transporting a firearm or dangerous weapon in a privately owned vehicle hidden from view, unless properly secured in the vehicles trunk as per paragraph 5.1.4.3. (Added).

5.1.3.3. (Added-AFMC) Designate secure facilities for storing privately owned firearms and develop accountability procedures. Establish storage procedures that ensure adequate protection.

5.1.3.4. (Added-AFMC) SF armories are not repositories for resources owned by other agencies, however, the installation commander may authorize (in writing) the storage of an agency's firearms and munitions in another agency's storage facility. Develop local procedures for the accountability, handling, inventory, issuing, and container and lock requisition (to include procedures for keys and combinations). Storage of cases, covers, boxes, and nonfirearm type items such as bows, arrows, swords, knives, scopes, nun chucks, etc., is discouraged.

5.1.3.5. (Added-AFMC) Develop local procedures for issue, receipt, and accountability. Implement controls for checking out weapons for specified periods of time, and employ measures to trace weapons not returned at the end of the checkout period.

5.1.3.6. (Added-AFMC) Inform base personnel of prohibitions regarding privately owned weapons through base in-processing briefings, bulletins, notices, commander's calls, visitor control centers, etc. Firearms and dangerous weapons prohibitions apply to civilian and military workers, members residing on base, visitors, contractors, subcontractors, etc.

5.1.3.6.1. (Added-AFMC) Require registration of all privately owned firearms stored on the installation with the security forces. Note: This includes firearms stored in MFH, whether located on or off the installation.

5.1.4. (Added-AFMC) Owner's responsibilities for privately-owned weapons:

5.1.4.1. (Added-AFMC) All personnel in the possession of firearms must comply with all federal, state, and local laws, ordinances, and military regulations on registering, storing, bearing, possessing, and using privately owned firearms. Register all privately owned firearms stored on AFMC installations with the SF. Registrant will indicate where the privately owned firearm is being stored.

5.1.4.2. (Added-AFMC) Except for certified LE officers performing official duties on the installation, anyone possessing a weapon, even if licensed by state or federal authority to possess and conceal a weapon, must follow the laws and regulations enforced by the installation.

5.1.4.3. (Added-AFMC) Carrying a concealed weapon on any part of the installation is prohibited unless conducting official (LE) duties, or unless authorized to do so by the installation commander. City, county, or state concealed weapon permits will not be honored in areas under exclusive federal jurisdiction, or in controlled areas. For areas of the installation under other types of jurisdiction, individuals carrying concealed weapons when not conducting official (LE) duties or without the installation commander's permission are subject to administrative sanctions. This includes, but is not limited to, barment from the installation. Transporting privately owned firearms on the installation is prohibited except to and from authorized storage or shooting areas. The

firearm must be cleared and safe, with the breech open. While transporting firearms, they will be placed in the trunk or in a securable compartment closest to the rear of the vehicle. Transporting firearms on bicycles, motorcycles, or on any other two or three wheeled vehicles is prohibited. Firearms will not be stowed in such a manner as to appear to be a concealed weapon, e.g., under seats or partially hidden. Ammunition must be stored and locked away separately.

5.1.5. (Added-AFMC) AF Form 1314, **Firearms Registration**. Complete this form for all privately owned firearms stored on the installation. This also includes all firearms stored in MFH by the residents. Annotate any visible damage to the weapon in the "MAKE (manufacture)" block. Continue on a separate sheet of paper, if additional space is required. Reaccomplish the form when additions or deletions are required.

5.1.5.1. (Added-AFMC) Original page of AF Form 1314 is forwarded to the individual's unit or the installation SF.

5.1.5.2. (Added-AFMC) Provide the owner of the weapon the first copy of the form.

5.1.5.3. (Added-AFMC) For dormitory residents: Forward the form's second copy (card) to the storage facility for safe keeping in the activity files. For housing area residents: Forward the second copy to the security forces section maintaining the privately owned database for keeping. Store those forms separate from the original AF Form 1314. To verify permanent removal of firearms when the owner leaves, this copy is sent to the individual's unit.

5.2. AA&E Facility Criteria. When constructing new AA&E facilities, follow the guidance in DoD 5100.76-M and AF Handbook 31 series. If the construction project is behind schedule, provide a copy of the revised contract to the MAJCOM/SP.

5.2. (Added-AFMC) Modifications to existing facilities storing arms, ammunition & explosives (AA&E) will follow guidance listed in DoD 5100.76-M and Mil-Handbook 1013/1. All facilities storing AA&E will be designed and constructed according to DoD 5100.76-M and Mil-Handbook 1013/1. Existing facilities, which were designed prior to November 1994, will be modified to provide a minimum of ten minutes forced entry delay. Structural upgrades to meet this design goal will follow Mil-Handbook 1013/1.

5.2.1. IDE Requirements. IDE is essential when protecting firearms. In addition to the standards outlined in DoD 5100.76-M, the following standards are mandatory:

- Equip the AA&E facility with a duress alarm system unless the weapons are within in a restricted area (as specified by AFI 31-101) containing Priority A resources. Use the AF Form 1473, **Gun and Equipment Room Inventory**, to document inventories.

NOTES:

The installation commander reviews situations on a case-by-case basis to determine whether facilities require duress alarms.

- When opening a facility daily, physically inventory all firearms each day. AA&E facilities staffed 24-hours per day and those frequently opened for shift change shall be inventoried every time custody changes. Conduct a 100 percent inventory in all other AA&E facilities when opened.

5.2.2. Designating AA&E Facilities. Designate all arms, ammunition and explosives storage facilities as controlled areas after getting the approval of the installation commander.

NOTE:

This requirement doesn't pertain to operational quantities of munitions.

5.3. Other Firearms Storage Protection Considerations. At least once each duty day, the owners or users must physically check unattended facilities by inspecting locks, hinges, doors and exterior walls.

5.3.1. Modifying AA&E Facilities. Any time you change the internal layout of a facility (for example, adding crates or moving weapons racks), notify the RPP manager to conduct a program review.

5.4. Exemptions to Protection Requirements. These devices are exempt from firearms protection requirements:

- Starter guns (models that individuals can't easily modify to fire actual projectiles).
- Pen flares.
- Ram set guns.
- Firearms demilitarized according to DoD 4160.21-M-1, *Defense Demilitarization Manual*, October 1991.

5.4.1. General officers will provide the necessary protection for weapons and munitions issued to them.

5.5. Entry to Firearms Storage Facilities, Containers, and Other Protection Requirements. Commanders designate, in writing, which personnel may gain authorized unescorted access to AA&E facilities.

5.5.1. Emergency Entry Procedures. Develop procedures for emergency entry into firearms storage facilities.

5.6. Emergency Power and Lighting Requirements. When issuing firearms routinely from firearms storage facilities, equip the facility with battery- or generator-powered emergency lighting. Be sure that the system automatically switches over when the primary power fails. Provide emergency lighting for the interior of storage facility, entrances, and issue windows.

5.6.1. The installation commander reviews situations on a case-by-case basis to determine whether facilities require emergency power and lighting.

5.7. Protection Policy for Nonnuclear Munitions Storage Areas (NMSA). Follow these munitions storage procedures whenever practical:

- Consolidate munitions within structures. Maintain them in a single on-base NMSA as specified in AFI 91-409, *Explosive Safety Standards*.
- Designate the NMSA site as a controlled area.
- Arm owners and users who perform entry control duties in accordance with DoD 5100.76-M or as determined by the RPEC.
- Use AECS to eliminate personnel entry controllers.

NOTE:

You don't have to arm personnel who respond infrequently to open the gates for periodic traffic if effective duress procedures are available. Don't arm personnel when entering the area to access stored weapons and munitions.

5.7.1. Physical Security Standards. For complete guidance on physical security standards, consult DoD 5100.76-M. Protect classified munitions in accordance with DoD 5100.76-M or DoD 5200.1-R, *Information Security Regulation*, Jun 86, or AFI 31-401, *Information Security Program Management*, whichever is more stringent.

5.7.2. Changing AA&E Levels. When NMSA personnel change levels of munitions and explosives or alter the NMSA's risk categories, the owner/user must notify the ICSP.

5.7.3. After Duty Hour Responsibility. At the end of their duty day, NMSA personnel contact security police to release protection responsibilities (if applicable). Pass on all pertinent information on changes in munitions levels and locations.

5.8. Protection Requirements for Operating Levels of Munitions. The RPEC determines how to protect minimum operational levels of certain munitions items (signal flares, starter cartridges, power supplies, impulse cartridges, explosive bolts, and so on) that pose no hazard in small quantities. Store these materials in accordance with the safety criteria for explosives. Don't exceed the operational level of a 5-day peacetime supply.

5.9. Air National Guard and Air Force Reserve Firearms Storage Facilities. For planning purposes, the Air Force classifies these facilities as "located on military installations:"

- Firearms storage facilities maintained by the Air National Guard and Air Force Reserve.
- Storage facilities located on fenced bases or fields.
- Other areas leased to the United States Government and licensed by the Secretary of the Air Force.

5.9.1. Category I Requirements. Don't allow Air National Guard and Air Force Reserve units to store Category I risk items. *EXCEPTION:* ANG and AFRES facilities on military installations with armed guard response capability.

5.10. Installed or In-Use Munitions. The Air Force considers any munitions installed in aircraft, parachutes, life support equipment, and so on as **in use.** Secure and protect these munitions as part of the weapons system in accordance with AFI 31-101. Other protection criteria in this chapter don't apply for these munitions.

5.10.1. Protecting Vehicle-Installed Weapons. Maintain weapons under continuous surveillance unless physically secured to the vehicle by an approved lockable weapons rack. Refer to Table of Allowances 538, *Equipment for Security Police Activities*, for approved weapons racks.

5.10.1. (Added-AFMC) When using lockable vehicle weapons racks, follow the procedures below:

- Patrolmen will notify the LE desk when they leave their vehicle unattended.
- Weapons will not be permanently assigned to a vehicle and will be changed out at the end of each shift.

5.10.2. Protecting Aircraft Weapons. When removing a gun or pod from the aircraft, store it in the gun shop or other building with a lockable door and steel bars or equivalent barriers over the windows and other openings. Refer to DoD Manual 5100.76-M for lock specifications.

5.10.3. Protecting Aircraft Weapons Larger Then .50 Caliber. If the RPEC decides that indoor secure storage of aircraft weapons larger then .50 caliber is ineffective, follow at least one of these procedures:

- Store the weapons within a restricted or controlled area that has an entry controller.
- Ensure that the using agency assigns an individual to continuously monitor the weapons (this person must be knowledgeable and capable to sound an alarm).
- Inform the security police of the location of these large weapons so they can perform periodical checks.

5.10.4. Protecting Firearms on Aircraft. Park aircraft containing firearms cargo or having installed firearms on board in a restricted area if space is available. (See AFI 31-101.) You may park these aircraft in controlled areas if you can provide additional patrol coverage.

5.11. Nonappropriated Fund Activity Munitions. Each nonappropriated fund activity that stocks and sells small arms ammunition must establish written protection and accounting procedures.

5.11.1. Security police, fire protection, and explosives safety personnel review and approve these procedures.

NOTE:

Protect items identified as firearms and ammunition, stored and displayed in Army and Air Force Exchange System (AAFES) facilities for sale, according to the procedures prescribed in AAFES directives.

5.12. Control Keys and Locks. AA&E facility supervisors establish procedures for controlling keys (to include spares) to all locked structures, gates, and containers (except munitions maintenance and storage facilities specifically governed by AFI 21-101, *Single Manager for Modification, Major Maintenance, and Test Programs on Air Force Systems*. You may use a master key system (National Stock Number 5340-00-291-4214) for weapon racks inside an approved AA&E storage facility. Keys to AA&E storage buildings, rooms, and intrusion detection system must be maintained in accordance with DoD 5100.76-M.

5.13. (Added-AFMC) Some off-base movement of AA&E requires the protection of armed guard surveillance (AGS). Provide AGS when transporting category I weapons or munitions or when 16 or more (but less than 100) category II weapons or munitions are transported. When 50 or more category I or 100 category II weapons or munitions are transported off base two armed personnel are required. This policy can be waived by the Chief, Traffic Management Office (TMO) when weapons are being shipped by TMO under other federal or state guidelines which allow for alternative forms of secure movement of category I and II AA&E. In all cases, once category I and II AA&E are removed from an approved storage facility, they must never be left unattended or insecure. On-base movements require AGS for category I movements. When more than 50 category II weapons are moved (on base) AGS is required. NOTE: AGS is a one-armed guard and an unarmed driver, unless traveling off-installation with 50 category I or 100 category II weapons or munitions. AGS is then defined as two-armed guards.

5.13.1. (Added-AFMC) Category I and II weapons will be under constant surveillance when removed from their protective facilities. Individuals in possession of issued weapons are responsible for the security of this property while it is in their custody. The owning/using organization is responsible to provide an armed guard for 50 or more category II weapons while mobility processing. If 50 or more category II weapons are present during mobility processing, then an armed guard is required.

Chapter 6

PHYSICAL SECURITY OF SENSITIVE CONVENTIONAL ARMS, AMMUNITION, AND EXPLOSIVES (AA&E) AT CONTRACTOR-OPERATED LOCATIONS

6.1. Responsibilities of Air Force Contracting Activities. Maintain and follow DoD 5220.22-R, *Industrial Security Regulation,* December 85, and DoD 5100.76-M. Draw up appropriate contract provisions to ensure that contractors properly protect AA&E materials. For complete guidelines see Defense Federal Acquisition Regulation Supplement (DFARS) 223. 370, *Safety Precautions for Ammunition and Explosives,* 91/3, and the related clause in DFARS 252.223-7002, *Safety Precautions for Ammunition and Explosives,* 91/1.

6.1.1. Mandatory safety requirements for contractors are in DoD Manual 4145.26-M, *DoD Contractors' Safety Manual for Ammunitions and Explosives,* March 1996.

6.1.2. When commissioning contracted project is on a government-owned installation (including a GOCO industrial facility), include other requirements in the contract to supplement the requirements of DoD Manual 4145.26-M.

6.1.3. Review existing contracts containing AA&E requirements within 90 calendar days after this AFI's publication date to determine whether contractual modifications are necessary to protect AA&E items.

6.1.4. Report to Defense Investigative Service (DIS) any of the information specified in Appendix D of DoD 5100.76-M and update it if necessary.

6.2. Responsibilities of Contractor Administrative Offices. Air Force administrative offices must follow these procedures:

6.2.1. Maintain and follow DoD Regulation 5220.22-R and DoD Manual 5100.76-M.

6.2.2. Review contractor procedures to ensure that they comply with contractual requirements.

6.2.3. Approve contractor procedures in coordination with security personnel.

6.2.4. Send contractor reports of incidents involving all losses and theft of risk category AA&E to cognizant DIS Industrial Security Officer, the procuring contracting officer, and HQ AFSPA/SPLE, 8201 H Avenue SE, Kirtland AFB NM 87117-5664.

6.3. Responsibilities of the Contractor. Contractors must prepare written procedures in accordance with these regulations:

6.3.1. Comply with all required contract provisions (for example, DFARS 252.223-7002 and DoD Manual 4145.26-M).

6.3.2. Correct AA&E safety program deficiencies identified by the administrative contracting officer.

6.3.3. Report incidents according to approved procedures.

6.3.4. Comply with AFPD 24-2, *Preparation and Movement of USAF Material,* when contract provisions or approved procedures require contractors to ship AA&E to DoD facilities.

6.3.5. Dispose of unneeded AA&E according to approved procedures and instructions from the contracting officer.

Chapter 7

PROTECTING AIRFIELDS AND MISSION-SUPPORT AIRCRAFT

7.1. Controlled Areas: Designate these installation sectors as controlled areas:

- Flight lines.
- Mission-support aircraft parking areas.
- Maintenance hangars next to or in the immediate proximity of the flight line (particularly if aircraft periodically park in the hangars during nonduty hours). ***Note: Aircraft with a priority designation must follow the guidance in AFI 31-101.***
- Roadways leading to aircraft parking ramps and flight line hangers.

7.2. Protecting Distinguished Visitor (DV) Aircraft. When the DV is a Code 4 (3-star general or civilian equivalent) or above, follow these procedures:

- Park DV aircraft in a prominent area so maintenance personnel and security police patrols can closely monitor it.
- Park transient DV aircraft remaining overnight in an existing restricted area.
- Establish procedures to inform security police of the arrival, parking arrangements, and departure of all DV aircraft.

7.3. Safeguarding Classified Equipment on Aircraft. Follow DoD 5200.1-R/AFI 31-401 for specific policies on protecting classified equipment at USAF installations.

Chapter 8

PROTECTING FUNDS AND OTHER RESOURCES

8.1. General Guidelines. The standards and procedures outlined in this chapter apply to all Government funds. The installation commander must strongly encourage other activities not covered by this instruction to meet these protection requirements.

8.1.1. Defense Commissary Agency (DeCA), Services, and AAFES Facilities. DeCA, MWRS, and AAFES facilities must follow the protection requirements outlined in their manuals. Their requirements must provide protection at least equal to the standards prescribed here.

8.1.2. Post Offices. Encourage post offices located on bases in CONUS or in United States possessions to follow these requirements. Air Force posts offices operated by base information transfer centers must follow this instruction.

8.1.3. Controlling Negotiable Instruments. All Air Force personnel who control appropriated, nonappropriated, and other Government funds or negotiable instruments must follow this instruction. Provide the same protection as resalable merchandise for tickets held for resale at MWRS and AAFES facilities. The value of tickets held for resale does not affect total funds storage limitations.

8.1.4. Storing Negotiable Instruments. Store negotiable instruments such as blank checks, bonds, and money orders in a locked container, such as a safe or metal filing cabinet.

8.1.5. Area Designation for Fund Facilities. The RPEC determines whether to designate a controlled area to protect funds or resources with a total value under $100,000.

8.1.6. Storing High Cash-Value Items. Don't store funds, precious metals, jewels, or other items of high value in any container that stores classified material.

NOTE:

Protect items stocked in AAFES facilities for retail sale under the procedures prescribed in AAFES directives.

8.1.7. Protecting High Cash-Value Resources. In general, protect these resources according to their dollar value as prescribed by this chapter. The RPEC directs alternative protective measures when determining that these protection criteria are inappropriate in certain cases. Don't count these items when determining the total amount of funds for storage or escort purposes:

- United States Postal Services postage stamp stocks.
- Blank money orders, and Government pay checks.
- Negotiable instruments (checks) marked payable to the **United States Treasury,** stamped **For Deposit Only,** or made payable to an AFO or a nonappropriated fund instrumentality but not endorsed.

8.2. Fund Activity Custodian. Use the AF Form 439, **Robbery Checklist**. Follow these general guidelines:

- Protect funds according to local procedures established in the RPP.
- Establish written procedures for safeguarding funds and ensure that all employees comply.

- Reduce cash-on-hand to the lowest amount required for efficient operation.

8.2.1. Fund Escort Procedures. The funds activity custodian and the security police mutually develop escort methodology for Government funds locally and publish these procedures in the base resource protection regulation. The escort may be either from the fund activity or the security police. The installation may also contract an armored car service. Follow these guidelines when developing local fund escort procedures:

8.2.2. Use armed escorts for transporting funds or resources with a total value of more than $25,000. Conduct escorts during daylight hours whenever possible to help reduce risk.

8.2.3. The RPEC establishes the amount of funds, precious metals, jewels, or high-cash-value resources requiring escorts, when the total value is under $25,000. The RPEC assesses the local threat conditions and laws to determine the need for armed escorts. ***Note: Base this assessment on the dollar amount transported, protection resources available, threat, geographic location, distance, and transport route.***

8.3. Protection Measures for Central Depositories. Central depositories must follow procedures outlined for funds storage activities. (See paragraph **8.4.**)

8.4. Funds Storage Limits During Non-Operating Hours. The installation commander prescribes in writing the limits for storing funds during nonoperating hours.

8.4. (Added-AFMC) Installation commanders can delegate this to the Installation Chief of Security Forces.

8.4.1. Store funds under $100,000 in accordance with local RPEC guidelines.

8.4.2. Store funds exceeding $100,000 inside an approved alarmed vault or secure storage room with two levels of IDE. See AFMAN 31-224.

8.5. Fund Container Requirements and Procedures. Funds custodians must ensure containers used to store Government funds are certified as to their capability to protect funds. These containers must meet General Services Administration (GSA) specifications for funds storage. If the container does not meet GSA specifications, ensure it has a Underwriter's Laboratory (UL) label (or foreign equivalent) designating it a burglar-resistant safe. The use of previously approved containers now in use is acceptable.

8.5.1. Use of GSA-Approved Containers. Use GSA-approved security containers meeting Class 1 or higher specifications when storing $7,500 or more, except in central depositories. Containers that are manufactured to a GSA specification have an external label reading: "General Service Administration, Approved Security Container", and the manufactures name. Additionally, the container should have a fixed label stating the federal specification it was manufactured under and the protection it affords. Secure funds containers on casters or containers weighing less than 500 pounds without IDE (or not located inside a vault) to the premises.

8.5.2. Central Depository Requirements. A central depository is a centralized consolidated temporary funds storage facility operating as a convenience for small funds activities. Permanently established depositories must meet the following standards:

- Must be located where there is armed supervision.

- The person providing supervision will not have direct access to funds, keys, or container combinations.
- Must have an installed duress alarm that is connected to any 24-hour security police post.
- Funds custodians provide their own containers and must maintain positive control of lock combinations or keys.

8.5.3. Container Combination Control. Control the container combination and restrict it to the minimum number of persons. Change the combination:

- Every 6 months.
- When transferring, discharging, or separating personnel who have access to the container.
- When directed by the RPEC.

8.5.4. Storing Funds After Duty Hours. If storing more than $7,500 in a storage container at a cashier cage during nonoperating hours or in an isolated cash register during operating hours, follow these guidelines:

- Keep a packet of money (including foreign currency where applicable) separate from the rest of the stored funds.
- Place at least three $20 bills in the packet.
- Record the denomination, serial number, and series year (including letter suffix) of each bill.
- Store the record in a container separate from the one holding the funds or in a separate location from the funds.

8.6. Fund Storage Rooms. The installation commander selects hardened rooms for storing fund containers during nonoperating hours. The hardness of the designated fund-storage rooms depends on these factors:

- The value of the stored resources.
- The level of resistance against burglary provided by individual fund-storage containers.
- The presence of an IDE.

8.6.1. Fund Storage Room Protection Criteria. See applicable AF Handbook 31 series.

8.6.2. Protective Lighting. Provide interior and exterior lighting for all fund-storage facilities including facility entrances, corridors, and funds rooms.

NOTE:

Install switches for exterior lights in places that aren't accessible to unauthorized individuals.

8.6.3. Locks and Keys. Lock doors to fund storage rooms with, as a minimum, locks and hasps meeting MIL-P-17802 standards or a key-actuated dead bolt with at least a 1-inch throw. The owner or user develops written procedures for controlling keys. The security police resource protection manager must approve all key procedures.

8.6.4. Walls, Floors, and Ceilings. Reinforce walls, floors, and ceilings to provide penetration resistance equal to that of the doors and windows. Since this reinforcement can be expensive, planners should carefully select the location of funds activities or use IDE to compensate for construction deficiencies.

8.6.5. Using IDE. As an addition to IDE protection for unattended storage of funds, provide an IDE duress alarm to protect operational funds during operating hours. Planners may use duress alarm systems in:

- Central depositories.
- Walk-in vaults.
- Cashier cages.
- Base exchanges.
- Commissary checkout lines.

NOTE:

Not every checkout stand needs to have a duress alarm system. Planners determine how many checkout counters to equip with IDE by assessing the facility's location and floor plan.

8.6.6. IDE Failure. When IDE fails or malfunctions, the fund activity user must provide continuous surveillance of the funds. Perform this surveillance until the activity repairs the IDE or relocates the funds to an approved facility. The Fund activity user must have a way to sound the alarm for security police response to a theft attempt. *EXCEPTION:* If IDE fails or malfunctions in an AAFES and DeCa facility, the user conducts a physical inspection of the facility with security police. Attempt to reset the system twice. Secure the facility if the system doesn't reactivate. Security Police must conduct periodic checks of all funds facilities when the IDE isn't fully operational. Fund activity custodians initiate and review all IDE work orders.

8.7. Protecting Funds Under Field Conditions. Deployment commanders establish and enforce procedures for protecting Government funds in accordance with these guidelines.

8.8. Protecting Other Resources. Designate these sites or facilities as controlled areas:

- Command, Control, Communications and Computer (C4) Systems facilities, including air traffic control facilities, navigational aids (NAVAID) facilities, and off-base communication sites.
- SCIFs. For complete protection standards, see DCID 1/21.
- Bulk petroleum, oil, and lubricants storage areas.
- Liquid oxygen and hydrazine storage areas.

8.8.1. Postal Facilities. Designate postal facilities located outside the United States as controlled areas. The RPEC and security police assist postal managers in developing protective standards, on request. DoD 4525.6-M provides physical protection requirements for postal facilities.

8.8.2. Medical Facility Protection. Medical facility commanders negotiate the necessary host-tenant support agreements to support the medical facility protection program. Each medical facility must implement a protection program based on an assessment of its particular needs and resources, mission requirements, and local threats. Planners must follow these specific protection standards for hospital facilities:

- **Pharmacy.** Equip with IDE (one level) and duress alarms (IDE is either complete penetration or motion).
- **Emergency Room.** Equip with duress alarm.

- **Radioactive Medical Material.** Designate as a secure area.
- **Controlled Substances Storage.** Equip with one level of IDE and duress alarms.

8.8.3. Pharmacies and Controlled Substance Storage Areas. These areas require additional protection according to the Controlled Substance Act and Air Force supply directives. In addition to providing IDE protection, designate these facilities as controlled areas and harden them with:

- Double-locked doors.
- Metal screening or window.
- Reinforced walls, floors, and ceilings.

8.8.4. Protection Requirements for Controlled Substances Outside Pharmacies. Small quantities of controlled substances intended for immediate use and maintained in places outside the pharmacy (for example, in wards, emergency rooms, and treatment rooms) require additional precautions. Protect outside pharmacies in accordance with AFI 41-113, *Administration of Medical Activities*, and Air Force Manual 67-1, *USAF Supply Manual.*

8.8.5. Material Control Protection. Medical facility RPP must incorporate these procedures:

- Separate sensitive and accountable items from areas with heavy pedestrian traffic.
- Mark all equipment and pilferable supply items (for example, linens and operating uniforms).
- Store any weapons or munitions brought in by patients in approved storage containers.

8.8.6. Terrestrial Nuclear Reactors. Planners must devise a local system for obtaining security police response to reactor alarms when reactor personnel are off-duty. Implement these mandatory protection standards for all terrestrial nuclear reactors.

- Use Level II AECS for the reactor room, reactor control room, and areas containing reactor fuel.
- Provide two levels of alarms for the reactor control room and the reactor room.
- Use IDE for all doors leading to the reactor control room and the reactor room. Use solid-core construction for the control room and reactor room doors.
- Place a rod and bar grill on all openings larger than 96 square inches that aren't protected by IDE. See AFMAN 31-224, for grill specifications.
- Provide backup power for IDE.

NOTE:

For more information on protection standards for terrestrial nuclear reactors, see the applicable AFH 31 series.

8.8.7. Ground Wave Emergency Network (GWEN) Systems. GWEN systems are vital command and control communications systems during war. The GWEN system consists of a network or radio stations located near military installations which provide redundant routing for messages. HQ ACC/SPO coordinates site tasking letters with the parent MAJCOM. These letters assign the sites to the closest Air Force base and provide resource protection instructions.

8.8.7. (Added-AFMC) GWEN Systems. AFMC installations are assigned resource protection responsibility for GWEN sites located within their geographical area. HQ ACC/SFO is the tasking agency. AFMC/SF units will provide HQ AFMC/SFO a copy of their annual site surveys and reports.

Please forward NLT 30 days after completion of the review. Send to HQ AFMC - Office of Security Forces, 4225 Logistics Ave., Building 266, Room N208, Wright-Patterson AFB OH 45433-5760.

8.8.8. Mobile Maintenance Van (MMV). The maintenance contractor has primary responsibility for the MMV. Park the MMV on an installation when requested.

8.8.9. Over-the-Horizon-Backscatter (OTH-B) Radar. There are two similar systems: the East Coast Radar System and West Coast Radar System. Use a Level II AECS and one level of penetration IDE. Each facility must have a minimum of one entry controller or alarm monitor and one-person mobile patrol. This will be a contract force.

8.8.10. Protecting Other Controlled Areas. Coordinate controlled areas established by other Air Force directives with HQ AFSPA/SPLE and specify any unique physical protective measures. Outline these protection measures in the installations resources protection plan.

8.8.10.1. (Added-AFMC) Protection of Archaeological Sites. The base Civil Engineer or the base Environmental Management Office has responsibility to implement and manage an archaeological and historic preservation program.

8.8.10.2. (Added-AFMC) SF assist in this program by conducting resource protection site surveys; investigating vandalism and theft, and recommending specific protection and storage measures for identified resources.

8.8.10.3. (Added-AFMC) The Resource Protection Executive Committee (RPEC) takes positive protective measures when vandalism and theft become a problem. Protective measures may range from owner/user recognition and awareness to using a variety of supporting physical facilities such as lighting, fencing, and sensor systems. Care must be taken so that identification (signs, fences, lighting, etc) does not bring undo attention to an otherwise unrecognized resource or site.

Chapter 9

PROGRAM ADMINISTRATION

9.1. Deviations to the Resource Protection Program. Request approval for deviations from established criteria at the proper level of command and take compensatory measures.

9.1.1. AF Form 116. Use AF Form 116, **Request for Deviation from Security Criteria**, to document all deviations.

9.1.2. Deficiencies Within 10 Percent. Deficiencies within 10 percent of the standard and deficiencies that the responsible activity can correct within 60 days don't require a deviation request. The responsible activity must take compensatory measures for all deviations. Activities may not use blanket waivers for several different deficiencies.

NOTE:

Consolidate multiple deviations caused by a single deficiency on one AF Form 116.

9.1.3. Preparing AF Form 116. At the installation level, the responsible activity must prepare all deviation requests. Coordinate AF Form 116, with the ICSP. Activities may submit three kinds of requests:

- Temporary deviations (waivers) for 1 year. The approving authority may grant extensions after conducting a review.
- Permanent deviations (exceptions) for a 2-year period.
- Technical deviations (variances) for an indefinite period.

9.1.4. Review. The RPEC reviews each deviation annually. ***Note: For approval authority, see Paragraphs 1.6. and 1.7.***

9.1.5. Temporary Deviations. Temporary deviation requests must contain proposed compensatory measures.

9.1.6. Compensatory Measures. Compensatory measures compensate for the specific vulnerability created by the deficiency. Compensatory measures may cover:

- Additional protective forces
- Procedures
- Facilities
- Equipment (such as additional locks, IDE, lighting, or barricades) that meets this AFI's minimum protection standards.

9.2. RCS HAF-SP (AR) 7101, *Reporting of Significant Arms and Nonnuclear Munitions Losses and Incidents.* Commanders establish procedures to ensure lost, stolen, unaccountable, or recovered US government AA&E are reported to the ICSP. This includes, found, confiscated, or inventory adjustments. Immediately after discovering a significant incident, the ICSP notifies the servicing AFOSI and MAJCOM/SP by telephone. Refer to DoD Manual 5100.76-M for specific information regarding significant losses. Additionally, ICSP's must notify the local AFOSI unit anytime there is a confirmed loss, theft,

recovery, or inventory adjustment of any government-owned weapon regardless of whether the loss meets the criteria of "significant" as per DoD 5100.76-M.

9.2.1. Follow-Up Message. As soon as possible after telephone notification, the ICSP provides a follow-up report by message to the servicing AFOSI office, the MAJCOM/SP, HQ AFSPA/SPLE, and HQ USAF/SPO and LGMW (for incidents involving nonnuclear munitions). This follow-up report must reach HQ AFSPA/SPLE within 48 hours of the incident. HQ USAF/SPO will in turn notify OSD (C3I) DASD (CI) IS within 72 hours.

NOTE:

This paragraph also applies to COCO and GOCO facilities.

9.2.2. Reporting Procedures. Continue reporting under emergency conditions. Normal. Designate this report as emergency status and precedence code C-2. You may transmit during MINIMIZE.

9.2.3. Incident Reports. To ensure that all AA&E shipments are secure, the ICSP submits a copy of any incident report involving a commercial driver to HQ MTMC-MTSS, Columbia Pike, Falls Church VA 22041-5050 (CONUS ONLY). Report any installation incidents involving alcohol, drugs, or weapons.

9.2.4. Closing Reports. Submit closing reports on significant incidents when actions are final (command action taken, conviction, or investigation closed).

9.3. RCS: HAF-SP (A) 8301,*Report on the Protection of Arms, Ammunition, and Explosives (AA&E)*. The ICSP submits a two-part report annually to the parent MAJCOM/SP. The report consists of a completed AF Form 441, **Arms, Ammunition, and Explosives Report - Part 1, Losses, Thefts, and Recoveries**, and a facility criteria list (Part 2). The reporting period is 1 October through 30 September.

9.3. (Added-AFMC) Send RCS: HAF-SP (A) 8301 to HQ AFMC/SF by 12 January of each year.

9.3.1. Preparing AF Form 441. Use AF Form 441 to report significant thefts and recoveries (Part 1) and facility criteria status. Include a brief summary and status of all reportable AA&E incidents occurring during the reporting period. For each incident report, include the date of the occurrence, the type of incident (loss, recovery, or both), location, type of item (M16 rifle, 9mm ammunition, etc.), weapon serial number, model, and quantity. The ICSP sends the completed AF Form 441 to the MAJCOM/SP for consolidation. The MAJCOM/SP sends AF Form 441, Part 1, to HQ AFSPA/SPLE.

9.3.2. MAJCOM Priority List. MAJCOM establishes and monitors a priority list of AA&E facilities to meet the standards outlined in this instruction. For Part 2 of this report, the ICSP submits a facility criteria status list of all AA&E facilities. *EXCEPTION:* Don't include Category IV storage facilities. Only report facilities not meeting protection criteria. Provide comments explaining actions taken and programmed, estimated completion dates, and funding issues for all storage facilities. MAJCOM/SP keep Part 2.

9.3.3. Reporting Procedures. Continue reporting under emergency conditions. Normal. Designate this report as emergency status and precedence code C-2.

9.3.4. MAJCOM Reports. MAJCOM/SP submit consolidated reports to HQ AFSPA/SPLE. The MAJCOM report must reach HQ AFSPA/SPLE within 30 days following the close of the reporting period.

9.4. RCS: HAF/SP (M) 7601,*USAF Law Enforcement Report*. This report provides a system to obtain, analyze and maintain crime and offense data. Commanders use these reports to decide how to best use their resources to maintain order and discipline.

9.4.1. Preparing Reports. The ICSP provides this monthly report to the MAJCOM/SP not later than the 2nd day of the month with data of the previous month. MAJCOM/SP submits a consolidated report to HQ AFSPA/SPLE once per quarter but no later than the 7th day of the month.

9.4.2. Reporting Procedures. Designate this report as emergency status and precedence code C-2. Continue reporting under emergency conditions. Normal. You may transmit during MINIMIZE.

NOTE:

Provide the report data to the MAJCOM/SP by computer disk or electronic mail. MAJCOM/SP will use the same process to send data to HQ AFSPA/SPLE.

9.4.3. Using the Security Police Administration and Reports (SPAR) Program. Installation must use the SPAR program when compiling these reports. SPAR is a subprogram of the security police automated system (SPAS).

9.5. Visual Aids Prescribed. This instruction prescribes these visual aids:

- AFVA 31-201, **Installation Warning Sign (18 x 15)**
- AFVA 31-202, **Installation Warning Sign (36 x 30)**
- AFVA 31-203, **Controlled Area Sign (18 x 15)**
- AFVA 31-204, **Controlled Area Sign (36 x 30)**
- AFVA 31-205, **Controlled Area Sign (5 x 7)**

9.6. Forms Prescribed:

- AF Form 439, **Robbery Checklist**
- AF Form 440, **Bomb Threat Aid**
- AF Form 441, **Arms, Ammunition, and Explosives Report -**
- **Part 1, Losses, Thefts, and Recoveries**
- AF Form 1314, **Firearms Registration**
- AF Form 1473, **Gun and Equipment Room Inventory**
- AF Form 1608, **Emergency Numbers Telephone Decal**
- AF Form 1670, **Valuable Property Record**
- AF Form 2530, **Alarm System Test Record**
- DJFD Form 353, **Personal Identification**

NOTE:
Instructions for their use, preparation, and distribution is in other departmental or field publications.

CHAPTER 10 (ADDED-AFMC)

SECURING AUTOMATED DATA PROCESSING EQUIPMENT (ADPE)

10.1. (Added-AFMC) General Guidelines. The procedures for securing ADPE identified in this chapter apply primarily to desktop and laptop systems. Embedded computer systems have unique requirements spelled out in the appropriate directives. The RPEC should consider the following measures in developing and evaluating their ADPE security program. For the purposes of this chapter, "embedded" refers to nonprogrammable systems, which operate without human interface.

10.2. (Added-AFMC) Establishing a security program designed to protect ADPE. To ensure ADPE is adequately protected, a proper security program must be established, monitored, and improved through evaluation. Establishing and maintaining an adequate security program requires the accomplishment of prescribed steps. These steps are:

- Identification of the ADP assets (data, software, hardware, media, services, and supplies) requiring protection.
- Establishment of the value of each of the assets.
- Identification of the threat of theft associated with each of the assets.
- Identification of the vulnerability of the ADP system to these threats.
- Selection and implementation of security measures.
- Audit and refinement of the ADP security program on a continuing basis.

10.3. (Added-AFMC) Procedures for securing ADPE. The use of small, portable computer systems has become the standard in all operations. Due to the portability of these systems, the possibility of theft has increased proportionately. In light of this, it is imperative that owner/user personnel secure their ADPE to decrease the possibility of theft. Installation commanders and the RPEC must scrutinize the policies for the protection of these assets and ensure all possible means to reduce or eliminate theft are taken. The RPEC should consider the following measures in developing and evaluating their ADPE security program. Various combinations of these measures have proven effective in reducing the likelihood of ADPE theft.

- Locate the equipment within a secured building.
- Control access to prevent unauthorized people from using the equipment.
- Use entry authority lists when/where appropriate.
- Install an intrusion detection system (IDS) based upon the risk exposure as determined in para 10.2 and approved by the RPEC.
- To the maximum extent possible locate equipment in the following areas; a controlled area; areas that have limited entry, or in rooms that can be locked.
- Use locks, cables, or anchor pads which can "tie down" equipment to the work station, desk, or table.
- Store/secure components which are easily removed.
- If the ADPE is the portable type (laptop or notebook), secure the entire computer in a lockable storage cabinet.
- Lock the console or terminal keyboard when not in use.

- Use keyboard covers, which prevent access to the terminals.
- Place easily observed or readily identifiable identification marks on ADPE.
- Reduce/eliminate the number of after hour cleaning/repair people allowed access to areas containing ADPE.
- Conduct and record end of day checks of all areas containing ADPE to ensure equipment and the area is properly secured. SF 701, Activity Security Checklist, can be used for this purpose.
- Conduct inventory and adhere to accountability requirements outlined in AFI 33-112, Computer Systems Management.

10.4. (Added-AFMC) Forms Prescribed. AFMC Form 387 and AFMC Form 496.

STEPHEN C. MANNELL, Brig General, USAF
Chief of Security Police

Attachment 1

GLOSSARY OF ABBREVIATIONS, ACRONYMS AND TERMS

Abbreviations and Acronyms

AA&E—Arms, Ammunition, and Explosives

AAFES—Army and Air Force Exchange System

ACC—Air Combat Command

AECS—Advanced Entry Control System

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFO—Accounting and Finance Office

AFPD—Air Force Policy Directive

AFR—Air Force Regulation

AFRES—Air Force Reserve

AFVA—Air Force Visual Aid

ANG—Air National Guard

C4—Command, Control, Communications, and Computers

CIIDS—Commercial Interior Intrusion Detection System

COCO—Contractor-Owned, Contractor-Operated

CONUS—Continental United States

CPTED—Crime Prevention Through Environmental Design

DeCA—Defense Commissary Agency

DCID—Director of Central Intelligence Directive

DIS—Defense Investigative Service

DFARS—Defense Federal Acquisition Regulation Supplement

DoD—Department of Defense

DoDD—DoD Directive

DV—Distinguished Visitor

EECS—Electronic Entry Control Systems

FOUO—For Official Use Only

GSA—General Services Administration

GSU—Geographically Separated Unit

GWEN—Ground Wave Emergency Network

GOCO—Government-Owned, Contractor-Operated

HQ—Headquarters

HQ AFISA—HQ Air Force Intelligence Support Agency

HQ AFOSI—HQ Air Force Office of Special Investigations

HQ AFSPA—HQ Air Force Security Police Agency

HQ ESC—HQ Electronic Systems Center

HQ USAF/SP—HQ United States Air Force, Chief of Security Police

ICIDS—Integrated Commercial Intrusion Detection System

ICSP—Installation Chief of Security Police

IDE—Intrusion Detection Equipment

IRPP—Installation Resource Protection Plan

J-SIIDS—Joint-Service Interior Intrusion Detection System

MAJCOM—Major Command

MMV—Mobile Maintenance Van

MWRS—Morale, Welfare, Recreation and Services

NAVAID—Navigational Aids

NMSA—Nonnuclear Munitions Storage Areas

OTH-B—Over-the-Horizon-Backscatter Radar

RCS—Report Control Symbol

RPEC—Resource Protection Executive Committee

RPP—Resource Protection Program

SCI—Sensitive Compartmented Information

SCIF—SCI Facility

SP—Security Police

SPAR—Security Police Administration and Reports

SPAS—Security Police Automated Systems

UCMJ—Uniform Code of Military Justice

UL—Underwriter's Laboratory

Terms

These terms have standard usage throughout the USAF Resource Protection Program.—

Advanced Entry Control System (AECS)—A system to electronically control access to and from specific areas.

Air Force Base—A base supports Air Force units that consist of landing strips and all components of related facilities for which the Air Force has operating responsibility.

Base Comptroller System—The base system that links supply, comptroller, and military personnel flight.

Central Depository—Facility for the containers that base activities use to temporarily store funds.

Commercial Interior Intrusion Detection System (CIIDS)—CIIDS provides a physical security capability to support Air Force law enforcement personnel in meeting the requirements for alarm systems. CIIDS consists of three major elements: central monitor and control subsystem, data gathering panel, and sensors.

Crime Prevention Through Environmental Design (CPTED)—The environmental design or physical planning that bases implement to improve security in residential and commercial areas (Air Force facilities) by limiting criminal opportunity using physical barriers. CPTEDs primary goal is preventing crime and reducing the fear of crime. Bases maintain effective CPTED programs by evaluating existing or planned structures, determining how they relate to present and potential crime patterns, and recommending including design measures in cooperation with architects.

C4 Systems Facilities—Facilities that house C4 systems critical to the installation's mission or operation. Examples include automated data processing systems, communications systems, base wide local area network systems, and NAVAIDs, as well as utilities critical to operating these facilities.

Duress Alarm System—A mechanical or electronic device that enables personnel on duty to alert an agency (usually security police) to obtain immediate assistance without arousing suspicion.

Firearms—Any weapon (including starter guns) that individuals readily convert to expel a projectile through a barrel by the action of an explosive; the frame or receiver of any such weapon; and any firearm muffler or silencing device. This definition includes individual, crew-served, aircraft armament weapons, and pyrotechnic flare guns.

Firearms Storage Facility—Any structure approved by the installation commander for storing 30 or more Category IV (low-risk) weapons or any number of higher risk weapons.

Funds Activity—Any activity or function approved by the installation commander to handle funds. Consider branches or subactivities of a main function as separate fund activities.

Funds Container—Any receptacle that contains funds. This includes vaults, safes, cash boxes, or security containers.

Funds Custodian—The person designated to manage a funds activity.

Installation Computer Systems—Automated equipment that installations use to store, transmit, or process information (personnel data, funds data, equipment data, or classified material) in a digital format.

Integrated Commercial Intrusion Detection System (ICIDS)—The procurement of a commercial, physical security system including command, control and display, and zone subsystems from a United States Army-managed contract. The system is intended to satisfy physical security requirements throughout DoD.

Intrusion Detection Equipment (IDE)—Devices, subsystems, and systems used to detect and report intrusions into areas of security interest. Such equipment may employ a variety of techniques; i.e., mechanical, electronic, chemical, radiation, etc.

Joint-Services Interior Intrusion Detection System (J-SIIDS)—A family of DoD-approved IDE.

Night Depository.—Funds storage container constructed as an adjunct to the base banking facility or depositories constructed as a part of accounting and finance offices (AFOs).

Nonnuclear Munitions—A general term applied to nonnuclear explosives. It also refers to the filler of an explosive item. Exclude from the criteria established by this instruction any incendiary materials, for rocket motors that burn but don't explode.

Nonnuclear Munitions Storage Area (NMSA)—A designated area set aside for storing nonnuclear munitions. Consult AFI 31-101 when storing nonnuclear munitions within nuclear storage areas.

Nonnuclear Munitions Storage Facility—Any structure or location, except a designated storage area, storing nonnuclear munitions regularly or stockpiled.

Nuisance Alarm—Unexplained alarm activation - not caused by human error.

Owner or User—The person or office who has responsibility of the resource. This term doesn't apply to agencies that may have temporary responsibility for a resource (for example, transportation personnel handling in-transit AA&E).

Permanent Exception—The approved continuance of a noncorrectable condition that varies from a resource protection requirement. An exception requires compensatory measures.

Precious Metals—Refined silver, gold, platinum, palladium, iridium, rhodium, osmium, and ruthenium in bar, ingot, granulation, sponge, wire, or plate form.

Security Police Forces—Air Force military security police personnel (Air Force Specialty Codes 31PX/ 3P0X1/3P0X2) and all Department of the Air Force civilians, contract civilians, Air Force military augmenters and foreign national civilian personnel who have been designated by proper authority to perform guard or police duties within the meaning of Article 7b, Uniform Code of Military Justice (to be Air Force Doctrine Document 100); and paragraph 19a, Manual for Courts Martial 1969, revised.

Sensitive Compartmented Information Facility (SCIF)—A facility storing SCI in a formally accredited area, room, group of rooms, or an area where there is SCI discussion or electrically processing SCI. A SCIF may be permanent or temporary, mobile or fixed, and of varied construction. Locate SCIFs on United States Government-controlled facilities, contractor plants, or other civilian locations.

Signal Line Supervision—An active communications link that sends a continuous signal to allow operating personnel to detect immediately any simple breaks in the link. A continuous signal assures personnel that the system is operating correctly.

Technical Variance—The continuance of a nonstandard condition that technically varies from a requirement but provides essentially the same level of protection. A technical variance doesn't require activities to compensatory measures unless implementing the variance for a given facility or area would create a vulnerability in the protective system of the area.

Temporary Waiver—The approved continuance of a temporary condition that varies from a requirement. A temporary waiver requires compensatory measures.

Terminal Area—Remote computer that can access a computer facility.

USAF Resources—All property, equipment, facilities, and materials (classified or unclassified) within the jurisdiction, administration, or custody of the United States Air Force and its units, exclusive of those aerospace resources described in AFI 31-101. This definition includes both appropriated and nonappropriated resources.

Attachment 2

SAMPLE FORMAT FOR A LETTER OF EXPULSION

(Use Appropriate Letterhead)

FROM:

SUBJECT: Order Not To Enter or Reenter Military Reservation

TO:

1. It has come to my attention that you were involved in (state the incident) on (date).
2. Based upon these incidents of misconduct, I consider your continued presence on this installation to be detrimental to the maintenance of good order and discipline. Effective immediately, you are ordered not to enter (installation name) for a period of (state the time frame).
3. If you fail to comply with this order, you will be in violation of Title 18, United States Code, Section 1382, which reads in part:

   "Whoever reenters or is found within any installation, after having been removed therefrom or ordered not to reenter by any officer or person in command thereof, shall be fined not more than $500.00 or imprisoned for not more than six months or both."

4. Should you reenter (installation name) in violation of this order, without having received prior approval, you will be subject to detention by the military police for delivery to the appropriate civilian and military authorities.
5. If you are entitled to medical treatment at (state hospital name), you may enter (state installation name) to use said facility. To do so, you must present this letter to the security police personnel at the installation entry point and obtain the appropriate visitor pass.
6. This order will remain in effect for the period prescribed in Paragraph 2, unless otherwise revoked in writing by the Commander (state installation). If you desire reconsideration or modification of this order, you may present your justifications to me, in writing, through the Chief of Security Police.

Installation Commander's Signature Block

cc: SPS Reports and Admin Section

Attachment 3

POSSIBLE SITUATIONS REGARDING ENFORCEMENT OF ORDER WITHIN OR NEAR AIR FORCE INSTALLATIONS

Possible Situation	Action
1. Notice of impending or actual demonstration	Notify HQ USAF in accordance with JCS directives. Coordinate with local United States Attorney and other appropriate civil authorities. Review and write installation anti demonstration plans.
2. Peaceful demonstration outside perimeter of installation without interference to USAF mission	Ignore demonstrators while being alert to any change in status.
3. Demonstrators interfere with base operation to a minor degree, by obstructing traffic moving on- and off-base	Use alternate means of access. If necessary ask civil authorities to remove the obstruction. ***Note: Commanders are reminded that request for USAF assistance by civil authorities should be approved by Office of the Secretary of Defense before action of any kind is taken.***
4. Demonstrators cause serious interference with base operations and endanger USAF personnel or property.	Request assistance from civil authorities. If necessary, contact higher headquarters for instructions on the use of USAF resources. To protect USAF personnel and property, use the absolute minimum degree of force to restore order.
5. Demonstrators gain access to the installation proper.	Apprehend, issue a letter of expulsion (**Attachment 2**) and escort them off-base. If necessary ask local United States Marshals for assistance since they have the power of Federal arrest on United States government property.
6. After being ejected, demonstrators return or attempt to force their way into the installation.	Ask local federal and civil authorities to to control the demonstrators. If this control is beyond their capability, the commander uses whatever means possible to protect government personnel and property. The guiding principle here should be a minimum application of a force consistent with the restoration of order.

NOTE:

The guidance provided will be modified on a country by country basis in the overseas commands. International pact or bilateral agreements will provide local policy and guidance to handle civil disturbances and demonstrations.

Attachment 4
ENTRY POINT/PERIMETER SIGN

WARNING
UNITED STATES AIR FORCE PROPERTY

RESTRICTED PLANT

It is unlawful to enter this area without permission of plant security management. Unauthorized entry may lead to prosecution. While within this plant, all personnel and the property under their control are subject to search.

SECTION 21, INTERNAL SECURITY ACT OF 1950, 50 U.S. CODE 797

Attachment 5
INTERIOR PLANT CONTROLLED AREA SIGN

WARNING
CONTROLLED AREA

Entry is prohibited without the express permission of plant security management. Unauthorized entry may be cause for dismissal or prosecution under the provisions of Federal Law.

18 U.S. CODE 793

NO PHOTOGRAPHY